Processing an Intrusion on a PEO STAMIS System

Processing an intrusion of your system, contact the ACERT center using the Intrusion Response Checklist. Contact your PDISSO and the PEO STAMIS Information Assurance Officer, Mr. Greg Seitz 703-806-0507 to keep them informed of the progress and results. This report is on the ACERT web site at www.acert.belvoir.army.mil and you should be registered to receive the IAVA messages directly. PEO STAMIS will forward the IAVA's to the PDISSO's but all system and network administrators should be registered.

Intrusion Response Checklist

If you suspect or know a system is compromised, please follow these procedures and complete the form.

DON'T

Finger attempt to access the source, or contact the source.

Change the system files on the suspected/compromised system.

Connect to the system over the network.

DO

Unplug the machine from the network (if mission will allow).

Log-on as root at the console and do a complete dump of the system

Make sure you don't alter any files on the system.

Place the dump in a secure location.

Place the suspected/compromised system in a secure place. (Limit access to the system).

Complete the following and contact the ACERT at DSN 235-1113 or 1-703-706-1113:

Email the ACERT at: acert@liwa.belvoir.army.mil

Or contact RCERT CONUS at DSN 879-2482 or (520) 538-2482:

Email the RCERT at: rcert-conus@rcertc.army.mil

1. Report Originator Information: Date: _____________

a. Name ______________________ b. Rank/Grade _________________________

c. Unit/Post _____________ d. DSN Phone Number ________________________

e. Commercial Phone Number ______________

f. Position (system administrator, security manager, etc.) __________________________

g. MACOM ____________________ h. e-mail Address _________________________

i. Message Address __________________________

j. Mailing Address __________________________

____

____

2. Target Information (if additional targets use separate sheet):

a. Network Domain & Host Name (i.e., liwa.belvoir.army.mil) ______________________________

b. IP Address (i.e., 132.28.145.43) ____________________Subnet Mask____________________

c. Computer Model (i.e., Sun SPARCstation 10)____

d. Operating System/Version (SUN-OS 4.1.6 etc.) ____

e. Security Mode of Operation (dedicated, system high, multilevel etc.) ________________________

f. Security Classification (i.e., SBU, secret, etc.) ____

g. Network/System Mission (i.e., administration, C2, communications,

logistics, Domain Name Server, etc.) ____

h. Network Structure/Type ____

i. How Detected ____

j. Impact on Mission (if compromised) ____

k. AIS Auditing _______Yes________No___________Type______________________________

l. Firewall _____Yes ______No________Type____

m. IDS ______Yes _______No________Type ____

n. System Status ____________On-line ___________Off-line

3. Attack Session Information (correlates with the target information):

(if known, include; if unknown, leave blank and don't access system files)

a. Date/dates and time of the Session Start: __________________ Stop _______________________

b. Attack Method ____

c. Source IP____

d. Source Host & Netblock name if available) Host ________________Netblock___________________

e. Organization: (i.e.. fl3m, TheK) ____

f. Country: ____

4. Countermeasure(s) Installed (e.g., patches, TCP wrappers, shadow passwords, etc.)

a. Name and date installed: ____

(if known, include; if unknown, leave blank and don't access system files)

5. Brief Scenario (Description of incident)

____

____

____

____

____

____

____

____

____

____